TACACS+ Servers for AAA

This chapter describes how to configure TACACS+ servers used in AAA.

About TACACS+ Servers for AAA

The ASA supports TACACS+ server authentication with the following protocols: ASCII, PAP, CHAP, and MS-CHAPv1.

TACACS+ Attributes

The ASA provides support for TACACS+ attributes. TACACS+ attributes separate the functions of authentication, authorization, and accounting. The protocol supports two types of attributes: mandatory and optional. Both the server and client must understand a mandatory attribute, and the mandatory attribute must be applied to the user. An optional attribute may or may not be understood or used.

Note To use TACACS+ attributes, make sure that you have enabled AAA services on the NAS.

The following table lists supported TACACS+ authorization response attributes for cut-through-proxy connections.

Table 1: Supported TACACS+ Authorization Response Attributes

Attribute	Description
acl	Identifies a locally configured ACL to be applied to the connection.
idletime	Indicates the amount of inactivity in minutes that is allowed before the authenticated user session is terminated.

Attribute	Description
timeout	Specifies the absolute amount of time in minutes that authentication credentials remain active before the authenticated user session is terminated.

The following table lists supported TACACS+ accounting attributes.

.

Table 2: Supported TACACS+ Accounting Attributes

Attribute	Description
bytes_in	Specifies the number of input bytes transferred during this connection (stop records only).
bytes_out	Specifies the number of output bytes transferred during this connection (stop records only).
cmd	Defines the command executed (command accounting only).
disc-cause	Indicates the numeric code that identifies the reason for disconnecting (stop records only).
elapsed_time	Defines the elapsed time in seconds for the connection (stop records only).
foreign_ip	Specifies the IP address of the client for tunnel connections. Defines the address on the lowest security interface for cut-through-proxy connections.
local_ip	Specifies the IP address that the client connected to for tunnel connections. Defines the address on the highest security interface for cut-through-proxy connections.
NAS port	Contains a session ID for the connection.
packs_in	Specifies the number of input packets transferred during this connection.
packs_out	Specifies the number of output packets transferred during this connection.
priv-level	Set to the user privilege level for command accounting requests or to 1 otherwise.
rem_iddr	Indicates the IP address of the client.
service	Specifies the service used. Always set to “shell” for command accounting only.
task_id	Specifies a unique task ID for the accounting transaction.
username	Indicates the name of the user.

Guidelines for TACACS+ Servers for AAA

This section describes the guidelines and limitation that you should check before configuring TACACS+ servers for AAA.

IPv6

The AAA server can use either an IPv4 or IPv6 address.

Additional Guidelines

- You can have up to 200 server groups in single mode or 4 server groups per context in multiple mode.
- Each group can have up to 16 servers in single mode or 8 servers in multiple mode.
- For FPR1000, FPR2100, or FPR3100 Series that are running in ASA appliance mode, you must comply with these username conventions:
  - Must be Linux-valid usernames.
  - Must be lower-case only.
  - May include alphanumeric characters, period (.), or hyphen (-).
  - Must not include other special characters such as at sign (@) and slash (/).

Configure TACACS+ Servers

This section describes how to configure TACACS+ servers.

Procedure

Step 1 Configure TACACS+ Server Groups, on page 3.

Step 2 Add a TACACS+ Server to a Group, on page 5.

Configure TACACS+ Server Groups

If you want to use a TACACS+ server for authentication, authorization, or accounting, you must first create at least one TACACS+ server group and add one or more servers to each group. You identify TACACS+ server groups by name.

To add a TACACS+ server group, perform the following steps:

Procedure

Step 1 Identify the server group name and the protocol.

aaa-server *server_tag* **protocol tacacs+**

Example:

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

When you enter the **aaa-server protocol** command, you enter aaa-server group configuration mode.

Step 2 Specify the maximum number of failed AAA transactions with a AAA server in the group before trying the next server.

max-failed-attempts *number*

Example:

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

The *number* argument can range from 1 and 5. The default is 3.

If you configured a fallback method using the local database (for management access only), and all the servers in the group fail to respond, or their responses are invalid, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for a period of 10 minutes (by default), so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately. To change the unresponsive period from the default, see the **reactivation-mode** command in the next step.

If you do not have a fallback method, the ASA continues to retry the servers in the group.

Step 3 Specify the method (reactivation policy) by which failed servers in a group are reactivated.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

Example:

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

The **depletion** keyword reactivates failed servers only after all of the servers in the group are inactive.

The **deadtime** *minutes* keyword-argument pair specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers. Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses. The default is 10 minutes.

The **timed** keyword reactivates failed servers after 30 seconds of down time.

Step 4 Send accounting messages to all servers in the group.

accounting-mode simultaneous

Example:

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

To restore the default of sending messages only to the active server, enter the **accounting-mode single** command.

Example

The following example shows how to add one TACACS+ group with one primary and one backup server:

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

Add a TACACS+ Server to a Group

To add a TACACS+ server to a group, perform the following steps:

Procedure

Step 1 Identify the TACACS+ server and the server group to which it belongs.

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

Example:

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

If you do not specify an **(***interface_name***)**, then the ASA uses the **inside** interface by default.

The server can use either an IPv4 or an IPv6 address.

Step 2 Specify the timeout value for connection attempts to the server.

timeout *seconds*

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the interval defined on the **retry-interval** command) until the timeout is reached. If the number of consecutive failed transactions reaches the limit specified on the max-failed-attempts command in the AAA server group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.

Example:

```
ciscoasa(config-aaa-server-host)# timeout 15
```

Step 3 Specify the server port as port number 49, or the TCP port number used by the ASA to communicate with the TACACS+ server.

server-port *port_number*

Example:

```
ciscoasa(config-aaa-server-host)# server-port 49
```

Step 4 Specify the server secret value used to authenticate the NAS to the TACACS+ server.

key

Example:

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

This value is a case-sensitive, alphanumeric keyword of up to 127 characters, which is the same value as the key on the TACACS+ server. Any characters over 127 are ignored. The key is used between the client and the server to encrypt data between them and must be the same on both the client and server systems. The key cannot contain spaces, but other special characters are allowed.

Monitoring TACACS+ Servers for AAA

See the following commands for monitoring TACACS+ servers for AAA:

- **show aaa-server**

  This command shows the configured TACACS+ server statistics. Enter the **clear aaa-server statistics** command to clear the TACACS+ server statistics.

- **show running-config aaa-server**

  This command shows the TACACS+ server running configuration. Enter the **clear configure aaa-server**command to clear the TACACS+ server configuration.

History for TACACS+ Servers for AAA

Table 3: History for TACACS+ Servers for AAA

Feature Name	Platform Releases	Description
TACACS+ Servers	7.0(1)	Describes how to configure TACACS+ servers for AAA. We introduced the following commands: **aaa-server protocol**, **max-failed-attempts, reactivation-mode, accounting-mode simultaneous, aaa-server host, aaa authorization exec authentication-server**, **server-port, key**, **clear aaa-server statistics**, **clear configure aaa-server**, **show aaa-server**, **show running-config aaa-server**, **username**, **service-type**, **timeout**.
TACACS+ servers with IPv6 addresses for AAA	9.7(1)	You can now use either an IPv4 or IPv6 address for the AAA server.

Feature Name	Platform Releases	Description
Increased limits for AAA server groups and servers per group.	9.13(1)	You can configure more AAA server groups. In single context mode, you can configure 200 AAA server groups (the former limit was 100). In multiple context mode, you can configure 8 (the former limit was 4). In addition, in multiple context mode, you can configure 8 servers per group (the former limit was 4 servers per group). The single context mode per-group limit of 16 remains unchanged. We modified the following commands to accept these new limits: **aaa-server**, **aaa-server host**.